EXHIBIT 13

EXHIBIT B

Exhibit B

U.S. Patent No. 8,472,447 v. Arista Switches that Support Internet Group Management Protocol (IGMP) Snooping + Multi-chassis Link Aggregation (MLAG)

CLAIM 1	'447 PATENT V. ARISTA SWITCHES THAT SUPPORT IGMP SNOOPING + MLAG
1[A] An aggregation switch in a multi-chassis system for performing Internet Protocol (IP) multicast snooping, comprising:	To any extent the preamble is limiting, the Arista Switches that Support Internet Group Management Protocol (IGMP) Snooping + Multi-chassis Link Aggregation (MLAG) ("Arista Switches") constitute an aggregation switch in a multi-chassis system for performing Internet Protocol (IP) multicast snooping. **Arista MLAG** In order to utilize all interconnects in an active/active manner, Arista EOS now supports the MLAG feature. This allows one to interconnect two Arista 7000 Family switches and use them as one logical switch for the purpose of L2 protocols such as STP or LACP. Key Benefits of MLAG: • No wasted bandwidth with uplinks in Spanning Tree Blocking state • Allows you to design non-blocking networks • Maintains same level of resiliency with redundant paths available at all times • Two Arista 7000 Family network switches can be in an MLAG pair, increasing your network scalability by 2X *See Multi-Chassis Link Aggregation - (MLAG)*, ARISTA NETWORKS, https://www.arista.com/en/products/multi-chassis-link-aggregation-mlag, (last accessed April 30, 2021).

	IGMP Snooping IGMP snooping is a layer 2 switch process that extracts lists of hosts receiving multicast group traffic by monitoring IGMP network packets. The switch uses these lists to avoid flooding hosts with extraneous multicast traffic by sending group packets only to group members. Besides preventing local hosts from receiving traffic for groups they did not join, snooping prunes multicast traffic from links that do not contain IGMP clients. When snooping is enabled, a switch examines IGMP packets sent between hosts connected to network switches and multicast routers (mrouters). When a switch finds an IGMP report from a multicast group recipient, it adds the recipient's port to the group multicast list. When the switch receives an IGMP leave, it removes the recipient's port from the list. Groups are removed upon the group timer expiry. When the switch finds an IGMP query packet or PIM hello packet from a multicast router, it adds the router's port to the port list for all multicast groups. *See EOS 4.25.2F User Manual*, ARISTA NETWORKS, https://www.arista.com/en/um-eos/eos-igmp-and-igmp-snooping#concept_vxq_v5h_5mb (last accessed April 30, 2021).
1[B] a plurality of virtual fabric link (VFL) ports coupled to a VFL, wherein the VFL is connected to a remote aggregation switch, wherein the remote	The Arista Switches comprise a plurality of virtual fabric link (VFL) ports coupled to a VFL, wherein the VFL is connected to a remote aggregation switch, wherein the remote aggregation switch is active and in a separate physical chassis. The Arista Switches operating as MLAG peers contain a peer link (e.g., a virtual fabric link) that can contain a plurality of Ethernet interfaces (e.g., a plurality of virtual fabric link (VFL) ports coupled to a VFL).

aggregation switch is active and in a separate physical chassis;	**10.3.4.1 Configuring the MLAG Peers** Connecting two switches as MLAG peers requires the establishment of the peer link and an SVI that defines local and peer IP addresses on each switch. The peer link is composed of a LAG between the switches. When all devices that connect to the MLAG domain are dually connected to the switches through an MLAG, a peer link of two Ethernet interfaces is sufficient to handle MLAG control data and provide N+1 redundancy. When the domain connects to devices through only one MLAG peer, the peer link may require additional Ethernet interfaces to manage data traffic. *See EOS 4.25.2F User Manual*, ARISTA NETWORKS, https://www.arista.com/assets/data/pdf/user-manual/um-books/EOS-4.25.2F-Manual.pdf, at 925 (last accessed April 30, 2021). When the Arista Switches are in MLAG configuration, the MLAG peer switches (e.g., aggregation switches) are connected by a peer link (e.g., VFL).

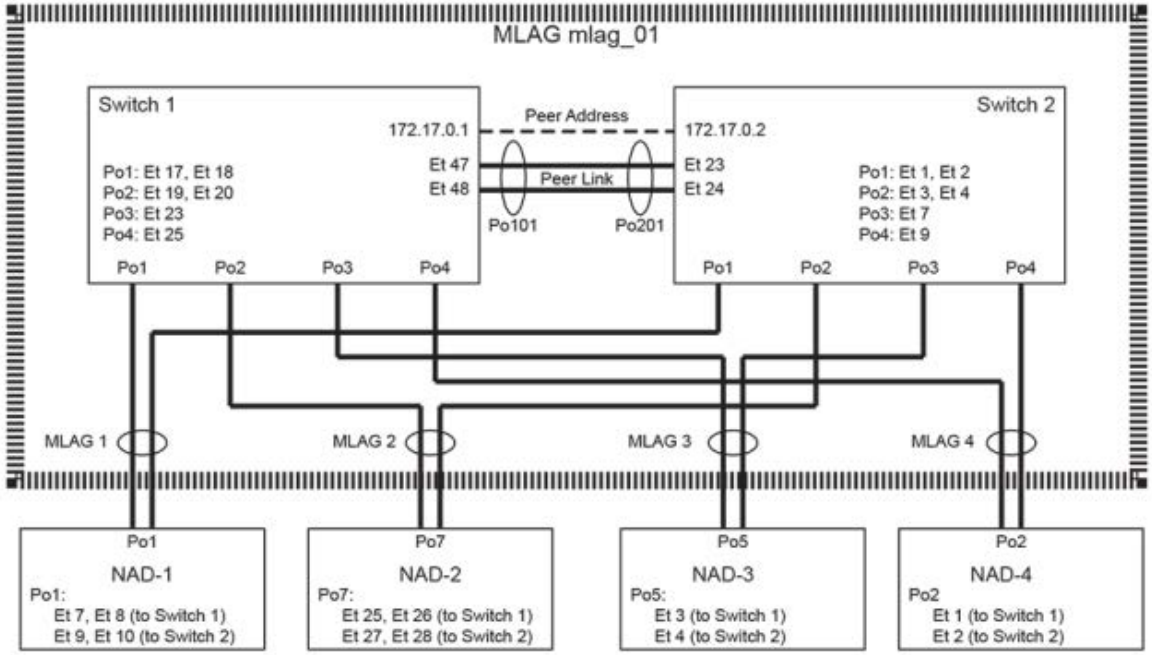
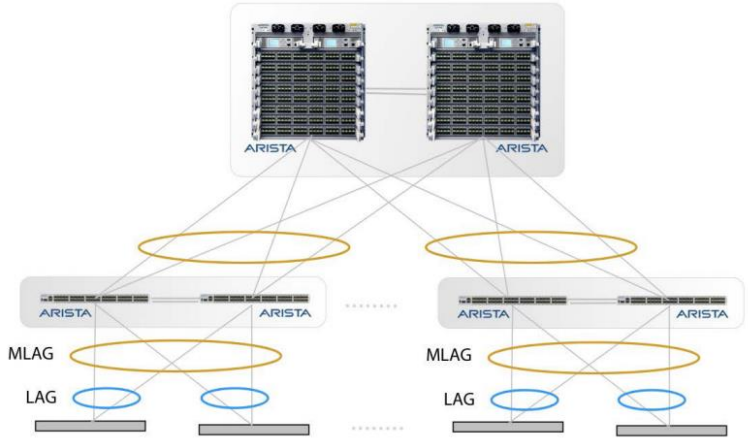


Figure 10: MLAG Implementation Example

See id. at 932.

The Arista Switches in MLAG configuration can be deployed at various places in the network. The MLAG peer switches are in a different physical chassis. The MLAG peer switches must be active for MLAG to work. If one of the peer switches is inactive, the other switch disables MLAG.



See Multi-Chassis Link Aggregation - (MLAG), ARISTA NETWORKS, https://www.arista.com/en/products/multi-chassis-link-aggregation-mlag (last accessed April 30, 2021).

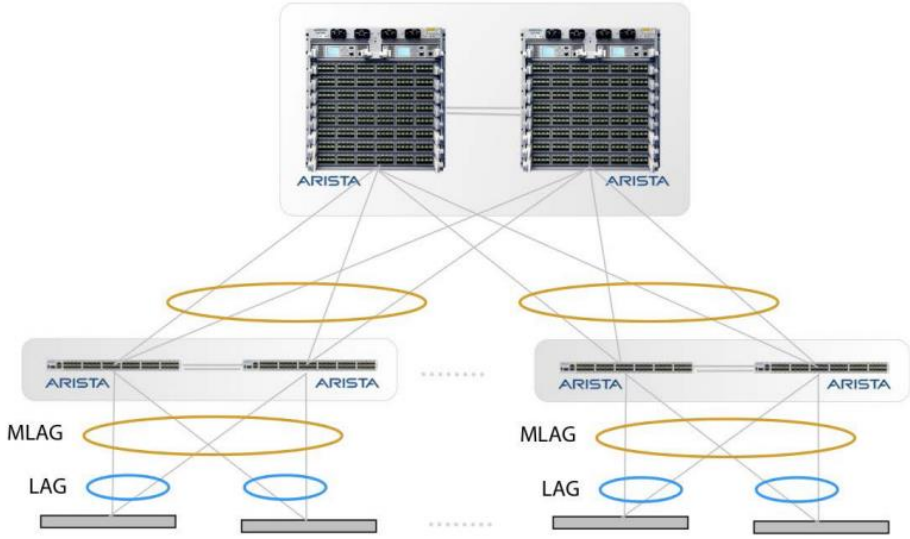
> **Guidelines**
>
> An MLAG is formed by connecting two switches through an interface called a peer link. The peer link carries control and data traffic between the switches, including advertisements and keepalive messages. This information coordinates the switches. Functioning peers are in the **active** state.

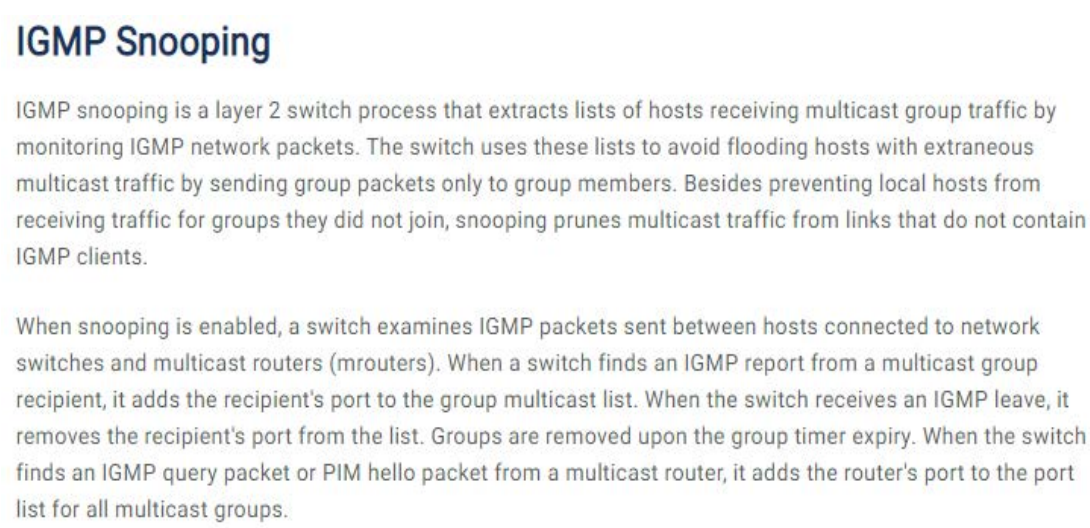
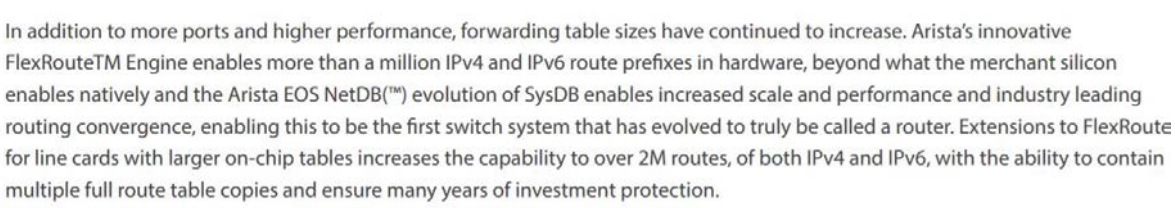
See EOS 4.25.2F User Manual, ARISTA NETWORKS, https://www.arista.com/assets/data/pdf/user-manual/um-books/EOS-4.25.2F-Manual.pdf, at 947 (last accessed April 30, 2021).

> ***10.3.4.1.2.6Heartbeat Interval and Timeout***
>
> The heartbeat interval specifies the period between the transmission of successive keepalive messages. Each MLAG switch transmits keepalive messages and monitors message reception from its peer. The heartbeat timeout is reset when the switch receives a keepalive message. If the heartbeat timeout expires, the switch disables MLAG under the premise that the peer switch is not functioning.

See id. at 928.

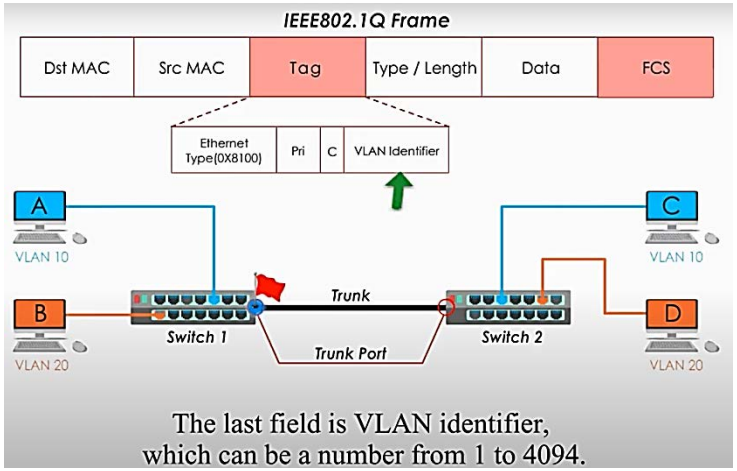
1[C] a plurality of external ports coupled to at least one edge node and at least one network node;	The Arista Switches comprise a plurality of external ports coupled to at least one edge node and at least one network node. The Arista Switches support multicast transmissions. The host nodes (e.g., network nodes) send IGMP packets to a multicast router to join or leave a multicast group. The Arista Switches examine these IGMP packets to extract information about hosts that want to join a multicast group. **Product Features** | **7500R** | **Licenses** **L2 FEATURES** Multi-chassis Link Aggregation (MLAG) | ✔ IGMP Snooping + MLAG | ✔ **MULTICAST FEATURES** IGMPv2 Snooping | ✔ IGMPv2 Querier | ✔ IGMPv3 Snooping | ✔ IGMPv3 Querier | ✔ *See Supported Features*, ARISTA NETWORKS, https://www.arista.com/en/support/product-documentation/supported-features (last accessed April 30, 2021). The Arista Switches in MLAG configuration are deployed at various places in the network wherein the network node is connected to the Arista Switches via an edge node.

	 *MLAG can be used at various places in the network to eliminate bottlenecks and provide resiliency.* *See Multi-Chassis Link Aggregation - (MLAG)*, ARISTA NETWORKS, https://www.arista.com/en/products/multi-chassis-link-aggregation-mlag(last accessed April 30, 2021).
1[D] a database maintaining IP multicast snooping information; and	The Arista Switches comprise a database maintaining IP multicast snooping information. The Arista Switches support multicast transmissions. The Arista Switches examine the IGMP join or leave packets to extract information about hosts that want to join the multicast group and the ports they are connected to (e.g.. snooping information). This extracted information is written to the group multicast list, which is stored in the on-chip memory on the switch (e.g.. storing the snooping information within a database). The switch uses this multicast list to forward multicast packets to nodes that joined the group and to prune multicast traffic from links that are not in the group.

	 *See EOS 4.25.2F User Manual*, ARISTA NETWORKS, https://www.arista.com/en/um-eos/eos-igmp-and-igmp-snooping#concept_vxq_v5h_5mb (last accessed April 30, 2021).  *See Arista 7500R Switch Architecture ('A day in the life of a packet')*, ARISTA NETWORKS, https://www.arista.com/assets/data/pdf/Whitepapers/Arista7500RSwitchArchitectureWP.pdf, at 3 (last accessed April 30, 2021).
1[E] a chassis management module for	The Arista Switches comprise a chassis management module for receiving the snooping information via at least the external ports, storing the snooping information within the database and sharing the snooping information substantially in real-time with the remote aggregation switch via the VFL.

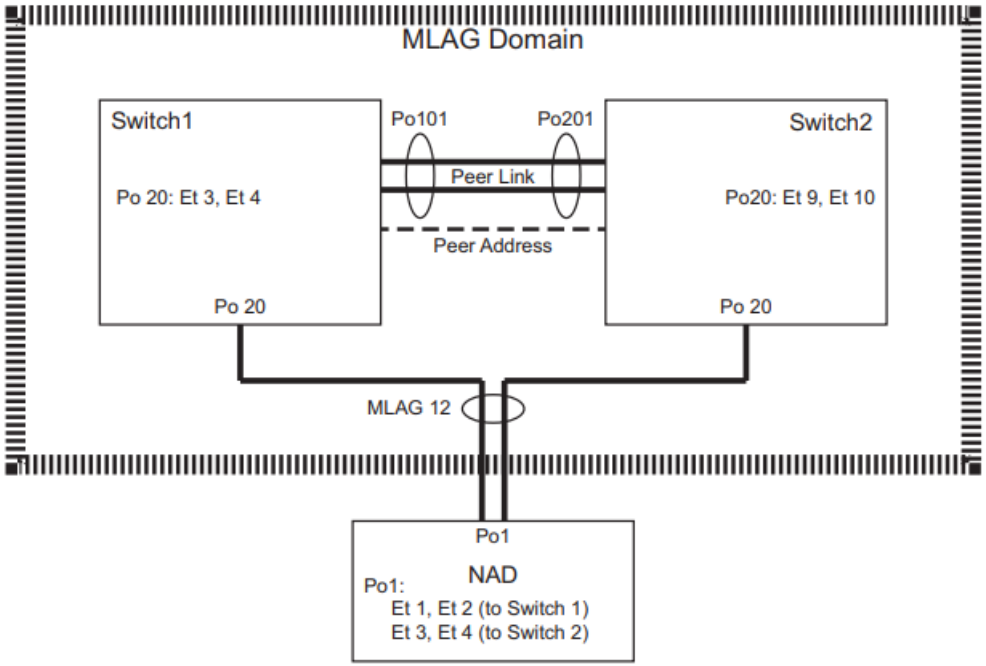
receiving the snooping information via at least the external ports, storing the snooping information within the database and sharing the snooping information substantially in real-time with the remote aggregation switch via the VFL;	The Arista Switches receive the IGMP packets (e.g., snooping information) sent from the host to a multicast router via the switches. The Arista Switches examine the IGMP packets to extract the snooping information and form the group multicast list. On information and belief, the Arista switches include a chassis management module to receive the IGMP packets, store the IGMP packets, and share the IGMP packets in real-time with the peer switches (e.g., remote aggregation switch) via the peer link (e.g., VFL). **15.2.4.2 IGMP Snooping** IGMP snooping is a layer 2 switch process that extracts lists of hosts receiving multicast group traffic by monitoring IGMP network packets. The switch uses these lists to avoid flooding hosts with extraneous multicast traffic by sending group packets only to group members. Besides preventing local hosts from receiving traffic for groups they did not join, snooping prunes multicast traffic from links that do not contain IGMP clients. When snooping is enabled, a switch examines IGMP packets sent between hosts connected to network switches and multicast routers (mrouters). When a switch finds an IGMP report from a multicast group recipient, it adds the recipient's port to the group multicast list. When the switch receives an IGMP leave, it removes the recipient's port from the list. Groups are removed upon the group timer expiry. When the switch finds an IGMP query packet or PIM hello packet from a multicast router, it adds the router's port to the port list for all multicast groups. *See EOS 4.25.2F User Manual*, ARISTA NETWORKS, https://www.arista.com/assets/data/pdf/user-manual/um-books/EOS-4.25.2F-Manual.pdf, at 2403 (last accessed April 30, 2021).
1[F] wherein the chassis management module further builds respective forwarding vectors for	The Arista Switches comprise a chassis management module, wherein the chassis management module further builds respective forwarding vectors for multicast traffic flows received from the at least one network node via the external ports or the VFL ports based on the snooping information. The Arista Switches receive the IGMP packets sent to a multicast router from hosts connected to the switches. The Arista Switches examine the IGMP packets to extract the snooping information and form the group multicast list (e.g., forwarding vector). On information and belief, the Arista Switches include a chassis management module to form the

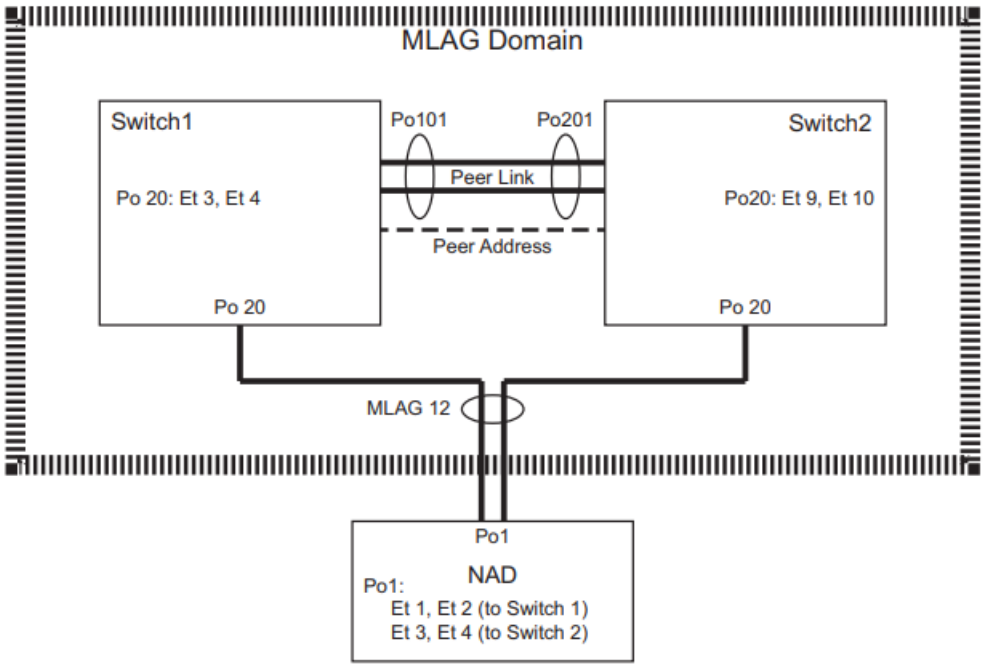
multicast traffic flows received from the at least one network node via the external ports or the [VFL] ports based on the snooping information;	group multicast list (e.g., build respective forwarding vectors for multicast traffic flows) received from the host node (e.g., network node) via the Ethernet interfaces (e.g., VFL ports). **15.2.4.2 IGMP Snooping** IGMP snooping is a layer 2 switch process that extracts lists of hosts receiving multicast group traffic by monitoring IGMP network packets. The switch uses these lists to avoid flooding hosts with extraneous multicast traffic by sending group packets only to group members. Besides preventing local hosts from receiving traffic for groups they did not join, snooping prunes multicast traffic from links that do not contain IGMP clients. When snooping is enabled, a switch examines IGMP packets sent between hosts connected to network switches and multicast routers (mrouters). When a switch finds an IGMP report from a multicast group recipient, it adds the recipient's port to the group multicast list. When the switch receives an IGMP leave, it removes the recipient's port from the list. Groups are removed upon the group timer expiry. When the switch finds an IGMP query packet or PIM hello packet from a multicast router, it adds the router's port to the port list for all multicast groups. *See id.*
1[G] wherein the chassis management module further determines a multicast index for a received multicast traffic flow to set-up hardware	The Arista Switches comprise a chassis management module wherein the chassis management module further determines a multicast index for a received multicast traffic flow to set-up hardware paths for forwarding the received multicast traffic flow to the external ports in a virtual local area network (VLAN) that requested the received multicast traffic flow via the at least one edge node, the multicast index being used globally between the aggregation switch and the remote aggregation switch. When a multicast frame from a network node that is part of a virtual local area network (VLAN) arrives at the Arista Switches' port, the multicast frame is tagged with a VLAN tag (e.g., multicast index) based on the VLAN that it belongs to. This VLAN tag enables the switch to set up a hardware path for forwarding the frame to a VLAN that the frame belongs to. On information and belief, the Arista Switches include a chassis management module to determine the VLAN tag (e.g., multicast index) for a received multicast traffic flow to set up hardware paths for forwarding the received multicast

paths for forwarding the received multicast traffic flow to the external ports in a virtual local area network (VLAN) that requested the received multicast traffic flow via the at least one edge node, the multicast index being used globally between the aggregation switch and the remote aggregation switch.	traffic flow to the external ports in a VLAN via an edge node. The VLAN tag (e.g., multicast index) is used globally between the aggregation switch and the remote aggregation switch.  *See*, *IEEE 802 1Q Tagging and Trunking 101*, SUNNY CLASSROOM, https://www.youtube.com/watch?v=vE5gvbmR8jg,, at 05:12 (last accessed May 3, 2021).
CLAIM 3	
3[A]. The aggregation switch of	To any extent the preamble is limiting, the Arista Switches comprise the aggregation switch of claim 1, wherein the snooping information includes at least one of group membership information identifying groups for receiving multicast traffic flows, queries for multicast traffic flows and identifiers of neighboring multicast routers.

claim 1, wherein the snooping information includes at least one of group membership information identifying groups for receiving multicast traffic flows, queries for multicast traffic flows, identifiers of multicast traffic flows and identifiers of neighboring multicast routers.	The Arista Switches examine the snooping information including the IGMP report/leave (e.g., group membership information) and IGMP query packet (e.g., queries for multicast traffic flows). The Arista Switches also add the multicast router's port to the port list (e.g., identifier of neighboring multicast routers) when the switches find an IGMP query packet or PIM hello packet. **15.2.4.2 IGMP Snooping** IGMP snooping is a layer 2 switch process that extracts lists of hosts receiving multicast group traffic by monitoring IGMP network packets. The switch uses these lists to avoid flooding hosts with extraneous multicast traffic by sending group packets only to group members. Besides preventing local hosts from receiving traffic for groups they did not join, snooping prunes multicast traffic from links that do not contain IGMP clients. When snooping is enabled, a switch examines IGMP packets sent between hosts connected to network switches and multicast routers (mrouters). When a switch finds an IGMP report from a multicast group recipient, it adds the recipient's port to the group multicast list. When the switch receives an IGMP leave, it removes the recipient's port from the list. Groups are removed upon the group timer expiry. When the switch finds an IGMP query packet or PIM hello packet from a multicast router, it adds the router's port to the port list for all multicast groups. *See EOS 4.25.2F User Manual*, ARISTA NETWORKS, https://www.arista.com/assets/data/pdf/user-manual/um-books/EOS-4.25.2F-Manual.pdf, at 2403 (last accessed April 30, 2021).
CLAIM 4	
4[A] The aggregation switch of claim 1,	To any extent the preamble is limiting, the Arista Switches comprise the aggregation switch of claim 1, wherein one or more of the external ports are member ports of a multi-chassis link aggregation group (MC-LAG) connected to an edge node.

wherein: one or more of the external ports are member ports of a multi-chassis link aggregation group (MC-LAG) connected to an edge node; and	As a non-limiting example in the configuration below, the port channels 20 of the Arista Switches associated with MLAG 12 (e.g., member ports of MC-LAG) are connected to the Network Attached Device (e.g., edge node). The port channels bundle the Ethernet interfaces of the peers.
	
	These Switch1 commands bundle Ethernet interfaces 3 and 4 in port channel 20, then associate that port channel with MLAG 12.
	
	`switch1(config)#interface ethernet 3-4`
	`switch1(config-if-et3-4)#channel-group 20 mode active`
	`switch1(config-if-et3-4)#interface port-channel 20`
	`switch1(config-if-po20)#mlag 12`
	`switch1(config-if-po20)#exit`
	`switch1(config)#`
	
	These Switch2 commands bundle Ethernet interfaces 9 and 10 in port channel 20, then associate that port channel with MLAG 12.
	
	`switch2(config)#interface ethernet 9-10`
	`switch2(config-if-et9-10)#channel-group 20 mode active`
	`switch2(config-if-et9-10)#interface port-channel 20`
	`switch2(config-if-po20)#mlag 12`
	`switch2(config-if-po20)#exit`
	`switch2(config)#`
	
	See EOS 4.25.2F User Manual, ARISTA NETWORKS, https://www.arista.com/assets/data/pdf/user-manual/um-books/EOS-4.25.2F-Manual.pdf, at 930, 931 (last accessed April 30, 2021).

	 *See 4.25.2F User Manual*, ARISTA NETWORKS, https://www.arista.com/assets/data/pdf/user-manual/um-books/EOS-4.25.2F-Manual.pdf, at 931 (last accessed April 30, 2021).
4[B] the remote aggregation switch includes one or more of the member ports	The Arista Switches comprise the aggregation switch of claim 1, wherein the remote aggregation switch includes one or more of the member ports of the MC-LAG. As a non-limiting example in the configuration below, switch2 (e.g., remote aggregation switch) includes port channel 20 of the MLAG 12 (e.g., MC-LAG). The port channel 20 of switch 2 bundles Ethernet interfaces 9 and 10.

of the MC-LAG.	These Switch2 commands bundle Ethernet interfaces 9 and 10 in port channel 20, then associate that port channel with MLAG 12.
	`switch2(config)#interface ethernet 9-10`
	`switch2(config-if-et9-10)#channel-group 20 mode active`
	`switch2(config-if-et9-10)#interface port-channel 20`
	`switch2(config-if-po20)#mlag 12`
	`switch2(config-if-po20)#exit`
	`switch2(config)#`
	
	See id. at 931.
	
	 
	
	See id. at 931.

CLAIM 5	
5[A] The aggregation switch of claim 4, wherein the chassis management module further receives a portion of the snooping information from the remote aggregation switch via the VFL, the portion of the snooping information having remote hardware device information associated therewith, the remote hardware device	To any extent the preamble is limiting, the Arista Switches comprise the aggregation switch of claim 4, wherein the chassis management module further receives a portion of the snooping information from the remote aggregation switch via the VFL, the portion of the snooping information having remote hardware device information associated therewith, the remote hardware device information including a remote external port identifier of a remote external port that received the snooping information on the remote aggregation switch. In the Arista Switches, the snooping information including the unicast and multicast MAC addresses are synchronized between the MLAG peers. Answered on September 26, 2015 2:29 am IGMP snooping is responsible for installing multicast mac addresses in the mac address table. In MLAG, the unicast and multicast mac addresses are synchronized between the MLAG peers. If a snooping entry exists on an MLAG port-channel, traffic destined to that group will be sent to that MLAG port-channel from either peer switch. The decision of which switch to forward this traffic is made by an upstream device and its hashing. Once traffic arrives on one of the MLAG peers, we will always try to forward it out a local interface, if possible. Only once a mac address is learned on a non-MLAG port-channel or on a port-channel where the local interfaces are down, do we use the peer-link for forwarding. *See IGMPSnooping in MLAG*, ARISTA NETWORKS, https://eos.arista.com/forum/igmpsnooping-in-mlag/ (last accessed April 30, 2021). The Arista Switches include a chassis management module to receive the snooping information from the remote aggregation switch via the peer link (e.g., VFL).

information including a remote external port identifier of a remote external port that received the snooping information on the remote aggregation switch.	A multi-chassis link aggregation group (MLAG) is a pair of links that terminate on two cooperating switches and appear as an ordinary link aggregation group (LAG). The cooperating switches are MLAG peer switches and communicate through an interface called a peer link. While the peer link's primary purpose is exchanging MLAG control information between peer switches, it also carries data traffic from devices that are attached to only one MLAG peer and have no alternative path. An MLAG domain consists of the peer switches and the control links that connect the switches. *See EOS 4.25.2F User Manual*, ARISTA NETWORKS, https://www.arista.com/assets/data/pdf/user-manual/um-books/EOS-4.25.2F-Manual.pdf, at 920 (last accessed April 30, 2021). In the Arista Switches, the snooping information shared by the remote aggregation switch includes the unicast and multicast MAC addresses that are mapped with the respective MLAG port channels (e.g., remote hardware device information). Answered on September 26, 2015 2:29 am IGMP snooping is responsible for installing multicast mac addresses in the mac address table. In MLAG, the unicast and multicast mac addresses are synchronized between the MLAG peers. If a snooping entry exists on an MLAG port-channel, traffic destined to that group will be sent to that MLAG port-channel from either peer switch. The decision of which switch to forward this traffic is made by an upstream device and its hashing. Once traffic arrives on one of the MLAG peers, we will always try to forward it out a local interface, if possible. Only once a mac address is learned on a non-MLAG port-channel or on a port-channel where the local interfaces are down, do we use the peer-link for forwarding. *See IGMPSnooping in MLAG*, ARISTA NETWORKS, https://eos.arista.com/forum/igmpsnooping-in-mlag/ (last accessed April 30, 2021). **show mac address-table mlag-peer** The **show mac-address-table mlag-peer** command displays the specified MAC address table entries learned from the MLAG peer switch.

Command Syntax

```
show mac address-table mlag-peer [ENTRY_TYPE] [MAC_ADDR] [INTF_1 ...
INTF_N] [VLANS]
```

INTF_X command filters display by port list. When parameter lists multiple interfaces, command displays all entries containing at least one listed interface.

- <no parameter> all Ethernet and port channel interfaces.
- **ethernet** *e_range* Ethernet interfaces specified by *e_range*.
- **port-channel** *p_range* Port channel interfaces specified by *p_range*.

See EOS 4.25.2F User Manual, ARISTA NETWORKS, https://www.arista.com/assets/data/pdf/user-manual/um-books/EOS-4.25.2F-Manual.pdf, at 1046 (last accessed April 30, 2021).

In MLAG, the snooping entries including the unicast and multicast MAC addresses are mapped with the respective MLAG port channels on the aggregation switch (including the remote aggregation switch) that received the snooping information. The port channels are specified by the p_range.

Answered on September 26, 2015 2:29 am

IGMP snooping is responsible for installing multicast mac addresses in the mac address table. In MLAG, the unicast and multicast mac addresses are synchronized between the MLAG peers. If a snooping entry exists on an MLAG port-channel, traffic destined to that group will be sent to that MLAG port-channel from either peer switch. The decision of which switch to forward this traffic is made by an upstream device and its hashing. Once traffic arrives on one of the MLAG peers, we will always try to forward it out a local interface, if possible. Only once a mac address is learned on a non-MLAG port-channel or on a port-channel where the local interfaces are down, do we use the peer-link for forwarding.

See IGMPSnooping in MLAG, ARISTA NETWORKS, https://eos.arista.com/forum/igmpsnooping-in-mlag/ (last accessed April 30, 2021).

	show mac address-table mlag-peer The **show mac-address-table mlag-peer** command displays the specified MAC address table entries learned from the MLAG peer switch. **Command Syntax** `show mac address-table mlag-peer [ENTRY_TYPE] [MAC_ADDR] [INTF_1 ... INTF_N] [VLANS]` *INTF_X* command filters display by port list. When parameter lists multiple interfaces, command displays all entries containing at least one listed interface. • <no parameter> all Ethernet and port channel interfaces. • **ethernet** *e_range* Ethernet interfaces specified by *e_range*. • **port-channel** *p_range* Port channel interfaces specified by *p_range*. *See EOS 4.25.2F User Manual*, ARISTA NETWORKS, https://www.arista.com/assets/data/pdf/user-manual/um-books/EOS-4.25.2F-Manual.pdf, at 1046 (last accessed April 30, 2021).
CLAIM 12	
12[A] The aggregation switch of claim 1, wherein the chassis management module further builds the forwarding vector for the received	The Arista Switches comprise the aggregation switch of claim 1, wherein the chassis management module further builds the forwarding vector for the received multicast traffic flow based on the multicast index. The MAC address table is built and synchronized between the MLAG peers based on the VLAN, from which the forwarding vector is formed. On information and belief, the chassis management module builds the forwarding vector for the received multicast traffic flow based on the multicast index. **10.4.6.47 show mac address-table mlag-peer** The **show mac-address-table mlag-peer** command displays the specified MAC address table entries learned from the MLAG peer switch. **Command Syntax** `show mac address-table mlag-peer` [ENTRY_TYPE][MAC_ADDR][INTF_1 ... INTF_N][VLANS]

multicast traffic flow based on the multicast index.	• VLANS command filters display by VLAN. • *<no parameter>* all VLANs. • vlan *v_num* VLANs specified by *v_num*. *See id.*
CLAIM 13	
13[A] The aggregation switch of claim 1, wherein the aggregation switch is a primary switch and the remote aggregation switch is a secondary switch, and wherein the chassis management module on the primary switch allocates the multicast	To any extent the preamble is limiting, the Arista Switches comprise the aggregation switch of claim 1, wherein the aggregation switch is a primary switch and the remote aggregation switch is a secondary switch, and wherein the chassis management module on the primary switch allocates the multicast index for the received multicast traffic flow and shares the multicast index with the secondary switch. The Arista Switches can be configured in MLAG comprising Arista 2 (e.g., local aggregation switch) as a primary switch and Arista 1 (e.g., remote aggregation switch) as a secondary switch. A switch is selected as the primary MLAG peer switch if it has the lowest MAC address of the two peers. On information and belief, the primary switch includes a chassis management module. When a multicast frame from a network node that is part of a virtual local area network (VLAN) arrives at the Arista Switches' port, the multicast frame is tagged with a VLAN tag (e.g., multicast index) based on the VLAN that it belongs to. This information or tag enables the switch to set up a hardware path for forwarding the frame to a VLAN that the frame belongs to. Ports on both the switches in the MLAG can use the VLAN tag to make forwarding decisions. On information and belief, the Arista Switches include a chassis management module to allocate the multicast index for the received traffic flow and share the multicast index with the secondary switch. Victor – The primary MLAG peer is selected based on the lowest MAC address of the two peers, this address is selected and the most significant bit of the address is flipped making a link local multicast address, based on your output: Posted by Mark Berly Answered on September 30, 2014 8:44 pm

index for the received multicast traffic flow and shares the multicast index with the secondary switch.	*See MLAG Priorities*, ARISTA NETWORKS, https://eos.arista.com/forum/mlag-priorities/ (last accessed April 30, 2021). Arista2: Arista2#sh mlag det MLAG Detailed Status: State : primary State changes : 2 Last state change time : 0:00:25 ago Hardware ready : True Failover : False Last failover change time : never Secondary from failover : False primary-priority : 32767 Peer primary-priority : 32767 Peer MAC address : 00:0c:29:ce:f6:26 Arista1: Arista1#sh mlag det MLAG Detailed Status: State : secondary State changes : 4 Last state change time : 0:56:06 ago Hardware ready : True Failover : False Last failover change time : never Secondary from failover : False primary-priority : 32767 Peer primary-priority : 32767 Peer MAC address : 00:0c:29:92:5c:be *See id.*
CLAIM 14	
14[A] The aggregation switch of	To any extent the preamble is limiting, the Arista Switches comprise the aggregation switch of claim 1, wherein the aggregation switch is a secondary switch and the remote aggregation switch is a primary switch, and wherein the

claim 1, wherein the aggregation switch is a secondary switch and the remote aggregation switch is a primary switch, and wherein the chassis management module on the secondary switch is prevented from allocating the multicast index for the received multicast traffic flow and receives the multicast index from the primary switch.	chassis management module on the secondary switch is prevented from allocating the multicast index for the received multicast traffic flow and receives the multicast index from the primary switch. As a non-limiting example, Arista Switches can be configured in MLAG comprising Arista 1 (e.g., local aggregation switch) as a secondary switch and Arista 2 (e.g., remote aggregation switch) as a primary switch. A switch is selected as the primary MLAG peer switch if it has the lowest MAC address of the two peers. Arista 1 (e.g., secondary switch) includes a chassis management module. Victor – The primary MLAG peer is selected based on the lowest MAC address of the two peers, this address is selected and the most significant bit of the address is flipped making a link local multicast address, based on your output: Posted by Mark Berly Answered on September 30, 2014 8:44 pm Arista2: Arista2#sh mlag det MLAG Detailed Status: State : primary State changes : 2 Last state change time : 0:00:25 ago Hardware ready : True Failover : False Last failover change time : never Secondary from failover : False primary-priority : 32767 Peer primary-priority : 32767 Peer MAC address : 00:0c:29:ce:f6:26 Arista1: Arista1#sh mlag det MLAG Detailed Status: State : secondary State changes : 4 Last state change time : 0:56:06 ago Hardware ready : True Failover : False Last failover change time : never Secondary from failover : False primary-priority : 32767 Peer primary-priority : 32767 Peer MAC address : 00:0c:29:92:5c:be *See id.*

The MAC address tables including the VLAN information (e.g., multicast index) are synchronized between the MLAG peers. The table entries including the VLAN information from the primary switch are received by the secondary switch. The Arista Switches include a chassis management module to receive the multicast index from the primary switch.

Answered on September 26, 2015 2:29 am

IGMP snooping is responsible for installing multicast mac addresses in the mac address table. In MLAG, the unicast and multicast mac addresses are synchronized between the MLAG peers. If a snooping entry exists on an MLAG port-channel, traffic destined to that group will be sent to that MLAG port-channel from either peer switch. The decision of which switch to forward this traffic is made by an upstream device and its hashing. Once traffic arrives on one of the MLAG peers, we will always try to forward it out a local interface, if possible. Only once a mac address is learned on a non-MLAG port-channel or on a port-channel where the local interfaces are down, do we use the peer-link for forwarding.

See IGMPSnooping in MLAG, ARISTA NETWORKS, https://eos.arista.com/forum/igmpsnooping-in-mlag/ (last accessed April 30, 2021).

show mac address-table mlag-peer

The **show mac-address-table mlag-peer** command displays the specified MAC address table entries learned from the MLAG peer switch.

Command Syntax

```
show mac address-table mlag-peer [ENTRY_TYPE] [MAC_ADDR] [INTF_1 ...
INTF_N] [VLANS]
```

INTF_X command filters display by port list. When parameter lists multiple interfaces, command displays all entries containing at least one listed interface.

- <no parameter> all Ethernet and port channel interfaces.
- **ethernet** *e_range* Ethernet interfaces specified by *e_range*.
- **port-channel** *p_range* Port channel interfaces specified by *p_range*.

	See EOS 4.25.2F User Manual, ARISTA NETWORKS, https://www.arista.com/assets/data/pdf/user-manual/um-books/EOS-4.25.2F-Manual.pdf, at 1046 (last accessed April 30, 2021).
CLAIM 15	
15[A]. A method for performing Internet Protocol (IP) multicast snooping on an aggregation switch in a multi-chassis system, comprising:	To any extent the preamble is limiting, the Arista Switches practice a method for performing Internet Protocol (IP) multicast snooping on an aggregation switch in a multi-chassis system. The Arista Switches support multicast transmissions through IGMP, IGMP Snooping (e.g., IP multicast snooping) and PIM-SM. Product Features / 7500R / Licenses MULTICAST FEATURES IGMPv2 Snooping ✓ IGMPv2 Querier ✓ IGMPv3 Snooping ✓ IGMPv3 Querier ✓ *See Supported Features*, ARISTA NETWORKS, https://www.arista.com/en/support/product-documentation/supported-features (last accessed April 30, 2021). The Arista Switches examines IGMP packets sent from a host node to a multicast router to join or leave a multicast group (e.g., performing Internet Protocol (IP) multicast snooping) to extract information about hosts that want to join the multicast group, as well as the ports they are connected to.

IGMP Snooping

IGMP snooping is a layer 2 switch process that extracts lists of hosts receiving multicast group traffic by monitoring IGMP network packets. The switch uses these lists to avoid flooding hosts with extraneous multicast traffic by sending group packets only to group members. Besides preventing local hosts from receiving traffic for groups they did not join, snooping prunes multicast traffic from links that do not contain IGMP clients.

When snooping is enabled, a switch examines IGMP packets sent between hosts connected to network switches and multicast routers (mrouters). When a switch finds an IGMP report from a multicast group recipient, it adds the recipient's port to the group multicast list. When the switch receives an IGMP leave, it removes the recipient's port from the list. Groups are removed upon the group timer expiry. When the switch finds an IGMP query packet or PIM hello packet from a multicast router, it adds the router's port to the port list for all multicast groups.

See EOS 4.25.2F User Manual, ARISTA NETWORKS, https://www.arista.com/en/um-eos/eos-igmp-and-igmp-snooping#concept_vxq_v5h_5mb (last accessed April 30, 2021).

The Arista Switches also support a Multi-Chassis Link Aggregation (MLAG) feature, which allows interconnection of two Arista 7000 Family switches (e.g., an aggregation switch in a multi-chassis system) and for use as one logical switch. The Arista Switches further support MLAG to work in conjunction with IGMP snooping.

Arista MLAG

In order to utilize all interconnects in an active/active manner, Arista EOS now supports the MLAG feature. This allows one to interconnect two Arista 7000 Family switches and use them as one logical switch for the purpose of L2 protocols such as STP or LACP. Key Benefits of MLAG:

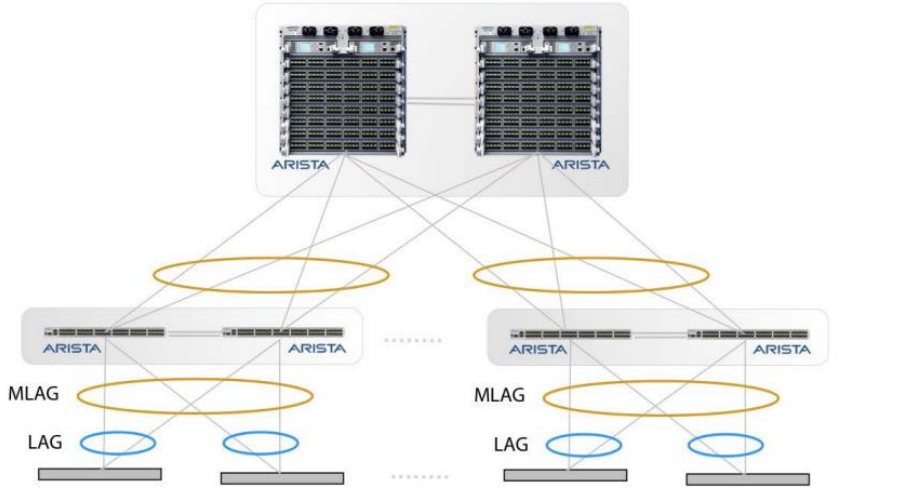
- No wasted bandwidth with uplinks in Spanning Tree Blocking state
- Allows you to design non-blocking networks
- Maintains same level of resiliency with redundant paths available at all times
- Two Arista 7000 Family network switches can be in an MLAG pair, increasing your network scalability by 2X

	See Multi-Chassis Link Aggregation - (MLAG), ARISTA NETWORKS, https://www.arista.com/en/products/multi-chassis-link-aggregation-mlag (last accessed April 30, 2021). *See Supported Features*, ARISTA NETWORKS, https://www.arista.com/en/support/product-documentation/supported-features (last accessed April 30, 2021).
15[B] receiving snooping information via at least external ports coupled to at least one edge node and at least one network node;	The method practiced by the Arista Switches comprises receiving snooping information via at least external ports coupled to at least one edge node and at least one network node. The Arista Switches support multicast transmissions. The host nodes (e.g., network nodes) send IGMP packets to a multicast router to join or leave a multicast group. The Arista Switches examine these IGMP packets to extract information about hosts that want to join a multicast group.

Product Features	7500R	Licenses
L2 FEATURES		
Multi-chassis Link Aggregation (MLAG)	✓	
IGMP Snooping + MLAG	✓	

Product Features	7500R	Licenses
L2 FEATURES		
Multi-chassis Link Aggregation (MLAG)	✓	
IGMP Snooping + MLAG	✓	
MULTICAST FEATURES		
IGMPv2 Snooping	✓	
IGMPv2 Querier	✓	
IGMPv3 Snooping	✓	
IGMPv3 Querier	✓	

	See Supported Features, ARISTA NETWORKS, https://www.arista.com/en/support/product-documentation/supported-features (last accessed April 30, 2021). **IGMP Snooping** IGMP snooping is a layer 2 switch process that extracts lists of hosts receiving multicast group traffic by monitoring IGMP network packets. The switch uses these lists to avoid flooding hosts with extraneous multicast traffic by sending group packets only to group members. Besides preventing local hosts from receiving traffic for groups they did not join, snooping prunes multicast traffic from links that do not contain IGMP clients. When snooping is enabled, a switch examines IGMP packets sent between hosts connected to network switches and multicast routers (mrouters). When a switch finds an IGMP report from a multicast group recipient, it adds the recipient's port to the group multicast list. When the switch receives an IGMP leave, it removes the recipient's port from the list. Groups are removed upon the group timer expiry. When the switch finds an IGMP query packet or PIM hello packet from a multicast router, it adds the router's port to the port list for all multicast groups. *See EOS 4.25.2F User Manual*, ARISTA NETWORKS, https://www.arista.com/en/um-eos/eos-igmp-and-igmp-snooping#concept_vxq_v5h_5mb (last accessed April 30, 2021). The Arista Switches in MLAG configuration are deployed at various places in the network wherein the network node is connected to the Arista Switches via an edge node.

	 *MLAG can be used at various places in the network to eliminate bottlenecks and provide resiliency.* *See Multi-Chassis Link Aggregation - (MLAG)*, ARISTA NETWORKS, https://www.arista.com/en/products/multi-chassis-link-aggregation-mlag, at 2 (last accessed April 30, 2021).
15[C] storing the snooping information within a database;	The method practiced by the Arista Switches comprises storing the snooping information within a database. The Arista Switches support multicast transmissions. The Arista Switches examine the IGMP join or leave packets to extract information about hosts that want to join the multicast group and the ports they are connected to (e.g., snooping information). This extracted information is written to the group multicast list, which is stored in the on-chip memory on the switch (e.g., storing the snooping information within a database). The switch uses this multicast list to forward multicast packets to nodes that joined the group and to prune multicast traffic from links that are not in the group.

IGMP Snooping

IGMP snooping is a layer 2 switch process that extracts lists of hosts receiving multicast group traffic by monitoring IGMP network packets. The switch uses these lists to avoid flooding hosts with extraneous multicast traffic by sending group packets only to group members. Besides preventing local hosts from receiving traffic for groups they did not join, snooping prunes multicast traffic from links that do not contain IGMP clients.

When snooping is enabled, a switch examines IGMP packets sent between hosts connected to network switches and multicast routers (mrouters). When a switch finds an IGMP report from a multicast group recipient, it adds the recipient's port to the group multicast list. When the switch receives an IGMP leave, it removes the recipient's port from the list. Groups are removed upon the group timer expiry. When the switch finds an IGMP query packet or PIM hello packet from a multicast router, it adds the router's port to the port list for all multicast groups.

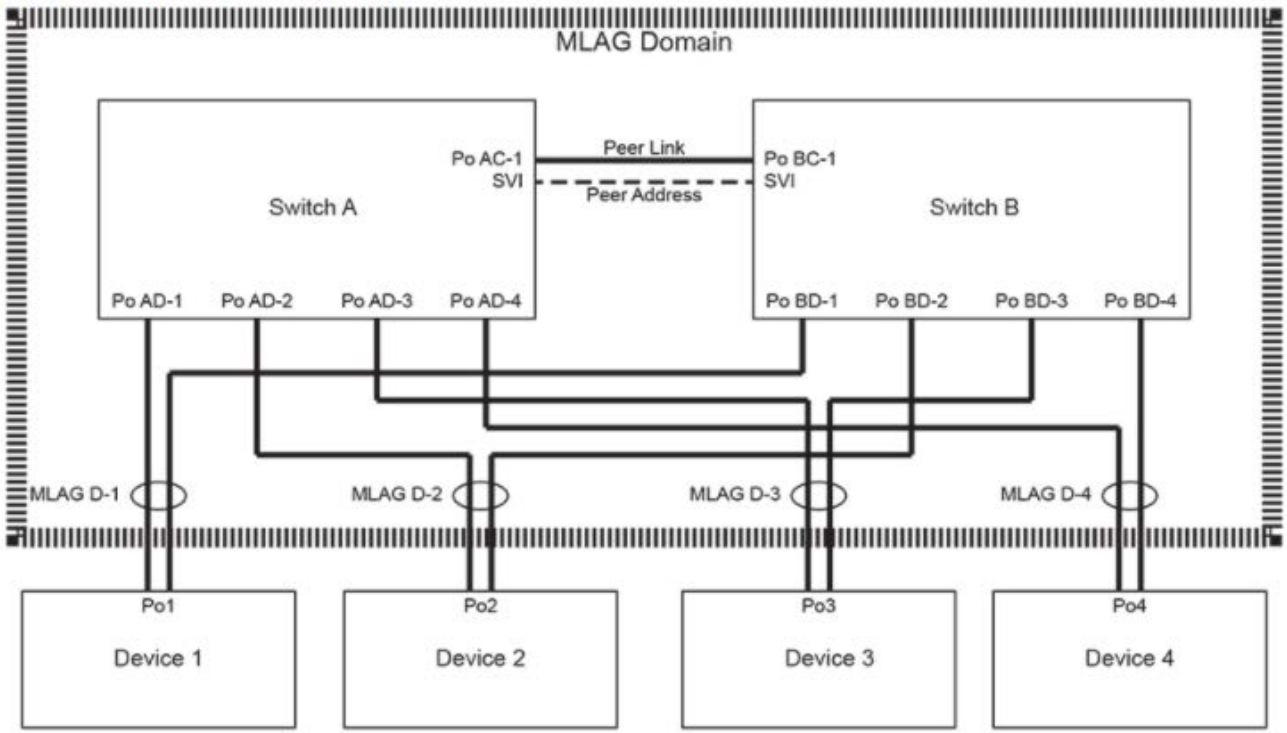
See EOS 4.25.2F User Manual, ARISTA NETWORKS, https://www.arista.com/en/um-eos/eos-igmp-and-igmp-snooping#concept_vxq_v5h_5mb (last accessed April 30, 2021).

In addition to more ports and higher performance, forwarding table sizes have continued to increase. Arista's innovative FlexRouteTM Engine enables more than a million IPv4 and IPv6 route prefixes in hardware, beyond what the merchant silicon enables natively and the Arista EOS NetDB(™) evolution of SysDB enables increased scale and performance and industry leading routing convergence, enabling this to be the first switch system that has evolved to truly be called a router. Extensions to FlexRoute for line cards with larger on-chip tables increases the capability to over 2M routes, of both IPv4 and IPv6, with the ability to contain multiple full route table copies and ensure many years of investment protection.

See Arista 7500R Switch Architecture ('A day in the life of a packet'), ARISTA NETWORKS, https://www.arista.com/assets/data/pdf/Whitepapers/Arista7500RSwitchArchitectureWP.pdf, at 3 (last accessed April 30, 2021).

15[D] sharing the snooping information substantially in real-time with a remote aggregation switch via a virtual fabric link (VFL) therebetween, wherein the remote aggregation switch is active and in a separate physical chassis	The method practiced by the Arista Switches comprises sharing the snooping information substantially in real-time with a remote aggregation switch via a virtual fabric link (VFL) therebetween, wherein the remote aggregation switch is active and in a separate physical chassis. The Arista Switches store the snooping information that is extracted from IGMP packets to the group multicast list. When the Arista Switches are in MLAG configuration, the MLAG peer switches (e.g., aggregation switches) are connected by a peer link (e.g., virtual fabric link (VFL)). This peer link acts as an interface for the two switches to communicate with each other, and the snooping information is synchronized over the peer link (e.g., sharing the snooping information substantially in real-time with a remote aggregation switch).

Figure 1. MLAG Domain Topology



A multi-chassis link aggregation group (MLAG) is a pair of links that terminate on two cooperating switches and appear as an ordinary link aggregation group (LAG). The cooperating switches are MLAG peer switches and communicate through an interface called a peer link. While the peer link's primary purpose is exchanging MLAG control information between peer switches, it also carries data traffic from devices that are attached to only one MLAG peer and have no alternative path. An MLAG domain consists of the peer switches and the control links that connect the switches.

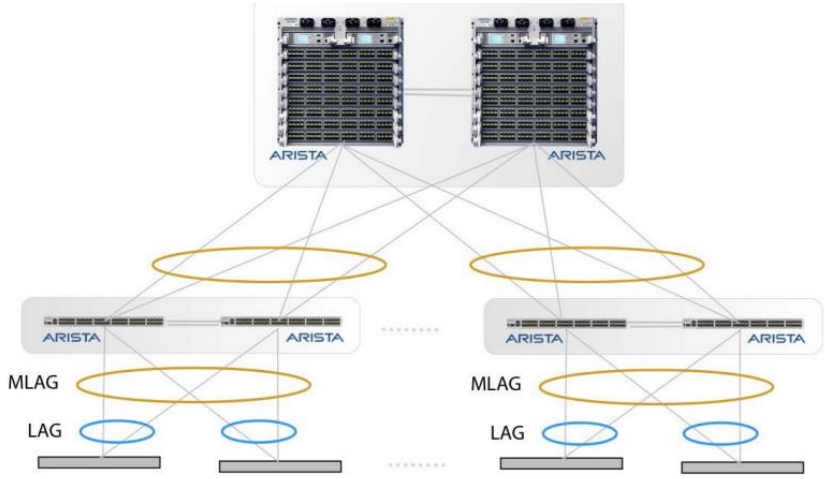
See EOS 4.25.2F User Manual, ARISTA NETWORKS, https://www.arista.com/en/um-eos/eos-multi-chassis-link-aggregation (last accessed April 30, 2021).

Answered on September 26, 2015 2:29 am

IGMP snooping is responsible for installing multicast mac addresses in the mac address table. In MLAG, the unicast and multicast mac addresses are synchronized between the MLAG peers. If a snooping entry exists on an MLAG port-channel, traffic destined to that group will be sent to that MLAG port-channel from either peer switch. The decision of which switch to forward this traffic is made by an upstream device and its hashing. Once traffic arrives on one of the MLAG peers, we will always try to forward it out a local interface, if possible. Only once a mac address is learned on a non-MLAG port-channel or on a port-channel where the local interfaces are down, do we use the peer-link for forwarding.

See IGMPSnooping in MLAG, ARISTA NETWORKS, https://eos.arista.com/forum/igmpsnooping-in-mlag/ (last accessed April 30, 2021).

The Arista Switches in MLAG configuration can be deployed at various places in the network. The MLAG peer switches are in different physical chassis. The MLAG peer switches must be active for MLAG to work. If one of the peer switches is inactive, the other switch disables MLAG.



MLAG can be used at various places in the network to eliminate bottlenecks and provide resiliency.

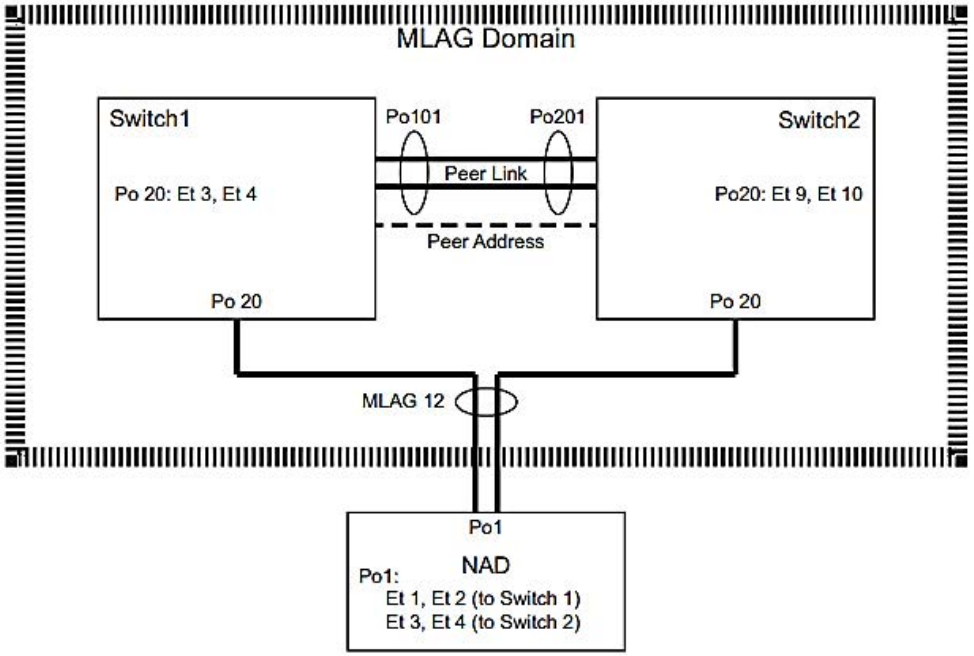
	See Multi-Chassis Link Aggregation - (MLAG), ARISTA NETWORKS, https://www.arista.com/en/products/multi-chassis-link-aggregation-mlag, at 2 (last accessed April 30, 2021). **Guidelines** An MLAG is formed by connecting two switches through an interface called a peer link. The peer link carries control and data traffic between the switches, including advertisements and keepalive messages. This information coordinates the switches. Functioning peers are in the **active** state. *See EOS 4.25.2F User Manual*, ARISTA NETWORKS, https://www.arista.com/assets/data/pdf/user-manual/um-books/EOS-4.25.2F-Manual.pdf, at 947 (last accessed April 30, 2021). ***10.3.4.1.2.6Heartbeat Interval and Timeout*** The heartbeat interval specifies the period between the transmission of successive keepalive messages. Each MLAG switch transmits keepalive messages and monitors message reception from its peer. The heartbeat timeout is reset when the switch receives a keepalive message. If the heartbeat timeout expires, the switch disables MLAG under the premise that the peer switch is not functioning. *See id.* at 928.
15[E] building respective forwarding vectors for multicast traffic flows received from the at least one network node based on the snooping	The method practiced by the Arista Switches comprises building respective forwarding vectors for multicast traffic flows received from the at least one network node based on the snooping information. The Arista Switches examine the IGMP join or leave packets to extract information about hosts (e.g., network nodes) that want to join multicast group. This extracted snooping information is used to build the group multicast list (e.g., the forwarding vector), which is stored in the switch. This multicast list includes information of various multicast groups, the network nodes that are a part of the group, and the port to which these nodes are connected. The MLAG peers use this multicast list (e.g., the forwarding vector) to forward multicast packets to the external ports that are connected to the nodes of the multicast group.

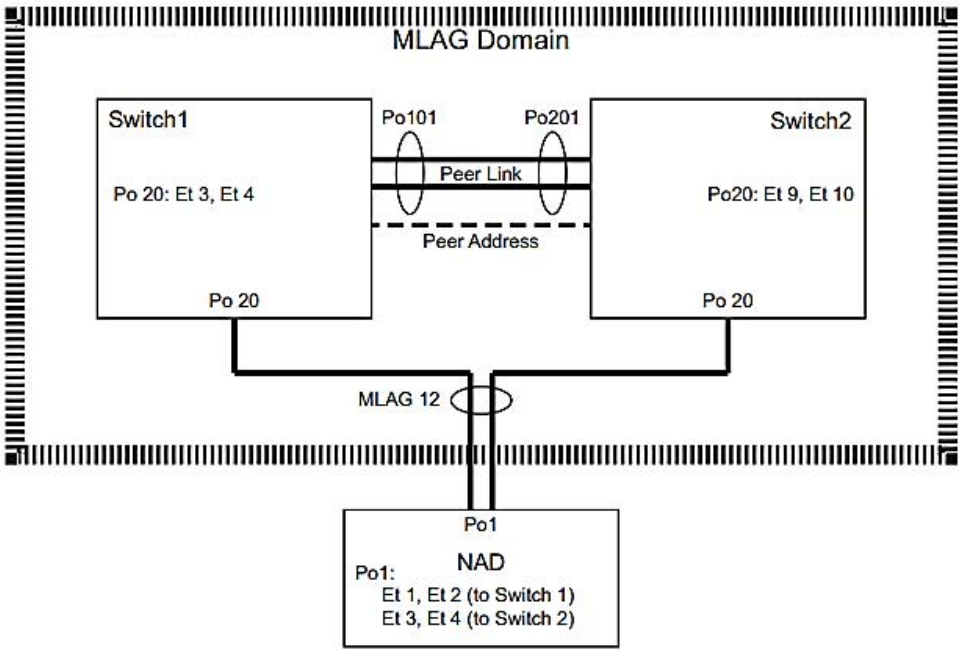
information; and	**15.2.4.2 IGMP Snooping** IGMP snooping is a layer 2 switch process that extracts lists of hosts receiving multicast group traffic by monitoring IGMP network packets. The switch uses these lists to avoid flooding hosts with extraneous multicast traffic by sending group packets only to group members. Besides preventing local hosts from receiving traffic for groups they did not join, snooping prunes multicast traffic from links that do not contain IGMP clients. When snooping is enabled, a switch examines IGMP packets sent between hosts connected to network switches and multicast routers (mrouters). When a switch finds an IGMP report from a multicast group recipient, it adds the recipient's port to the group multicast list. When the switch receives an IGMP leave, it removes the recipient's port from the list. Groups are removed upon the group timer expiry. When the switch finds an IGMP query packet or PIM hello packet from a multicast router, it adds the router's port to the port list for all multicast groups. *See id.* at 2403.
15[F] determining a multicast index for a received multicast traffic flow to set-up hardware paths for forwarding the received multicast traffic flow to the external ports in a virtual local	The method practiced by the Arista Switches comprises determining a multicast index for a received multicast traffic flow to set-up hardware paths for forwarding the received multicast traffic flow to the external ports in a virtual local area network (VLAN) that requested the received multicast traffic flow via the at least one edge node, the multicast index being used globally between the aggregation switch and the remote aggregation switch. The Arista Switches store the snooping information that is extracted from IGMP packets to the group multicast list. The switch uses this multicast list to forward multicast packets to nodes that joined the group and to prune multicast traffic from links that are not in the group.

area network (VLAN) that requested the received multicast traffic flow via the at least one edge node, the multicast index being used globally between the aggregation switch and the remote aggregation switch.	**15.2.4.2 IGMP Snooping** IGMP snooping is a layer 2 switch process that extracts lists of hosts receiving multicast group traffic by monitoring IGMP network packets. The switch uses these lists to avoid flooding hosts with extraneous multicast traffic by sending group packets only to group members. Besides preventing local hosts from receiving traffic for groups they did not join, snooping prunes multicast traffic from links that do not contain IGMP clients. When snooping is enabled, a switch examines IGMP packets sent between hosts connected to network switches and multicast routers (mrouters). When a switch finds an IGMP report from a multicast group recipient, it adds the recipient's port to the group multicast list. When the switch receives an IGMP leave, it removes the recipient's port from the list. Groups are removed upon the group timer expiry. When the switch finds an IGMP query packet or PIM hello packet from a multicast router, it adds the router's port to the port list for all multicast groups. *See id.* The Arista Switches support the IEEE 802.1Q standard. When a multicast frame from a network node which is part of a virtual local area network (VLAN) arrives at a port, the multicast frame is tagged with a VLAN tag (e.g., multicast index) based on the VLAN that it came from. This frame enables the switch to set up a hardware path for forwarding the frame to a VLAN that the frame belongs to (e.g., set-up hardware paths for forwarding the received multicast traffic). L2 FEATURES Product Features | 7500R | Licenses IEEE 802.1Q Trunking | ✔ *See Supported Features*, ARISTA NETWORKS, https://www.arista.com/en/support/product-documentation/supported-features (last accessed April 30, 2021). The ports on the switch use this VLAN tag to determine whether to forward the frame or not. If the frame is tagged for a VLAN that is connected to that port, the port forwards the frame. If the frame is tagged for a VLAN that is not

	connected to that port, the port drops the frame. Ports on both switches can use this tag to make forwarding decisions (e.g., being used globally between the aggregation switch and the remote aggregation switch) and this tag is removed once the frame reaches the egress port of either of the two switches. **11.3.3.2.2 Trunk Ports** Trunk ports carry traffic for multiple VLANs. Messages use tagged frames to specify the VLAN for which trunk ports process traffic. • The **`vlan trunk list`** specifies the VLANs for which the port handles tagged frames. The port drops any packets tagged for VLANs not in the VLAN list. *See EOS 4.25.2F User Manual*, ARISTA NETWORKS, https://www.arista.com/assets/data/pdf/user-manual/um-books/EOS-4.25.2F-Manual.pdf, at 1204 (last accessed April 30, 2021).
CLAIM 16	
16[A] The method of claim 15, wherein one or more of the external ports are member ports of a multi-chassis link aggregation group (MC-LAG) connected to an edge node and the remote	To any extent the preamble is limiting, the Arista Switches comprise the method of claim 15, wherein one or more of the external ports are member ports of a multi-chassis link aggregation group (MC-LAG) connected to an edge node and the remote aggregation switch includes one or more of the member ports of the MC-LAG connected to the edge node and wherein the receiving the snooping information further includes: receiving a portion of the snooping information from the remote aggregation switch via the VFL, the portion of the snooping information having remote hardware device information associated therewith, the remote hardware device information including a remote external port identifier of a remote external port that received the snooping information on the remote aggregation switch. In the configuration below, the port channels 20 of the Arista Switches associated with MLAG 12 (e.g., member ports of the MLAG) are connected to the Network Attached Device (e.g., edge node). The port channels bundle the Ethernet interfaces of the peers.

aggregation switch includes one or more of the member ports of the MC-LAG connected to the edge node and wherein the receiving the snooping information further includes: receiving a portion of the snooping information from the remote aggregation switch via the VFL, the portion of the snooping information having remote hardware device information associated	These Switch1 commands bundle Ethernet interfaces 3 and 4 in port channel 20, then associate that port channel with MLAG 12.
	`switch1(config)#interface ethernet 3-4`
	`switch1(config-if-et3-4)#channel-group 20 mode active`
	`switch1(config-if-et3-4)#interface port-channel 20`
	`switch1(config-if-po20)#mlag 12`
	`switch1(config-if-po20)#exit`
	`switch1(config)#`
	These Switch2 commands bundle Ethernet interfaces 9 and 10 in port channel 20, then associate that port channel with MLAG 12.
	`switch2(config)#interface ethernet 9-10`
	`switch2(config-if-et9-10)#channel-group 20 mode active`
	`switch2(config-if-et9-10)#interface port-channel 20`
	`switch2(config-if-po20)#mlag 12`
	`switch2(config-if-po20)#exit`
	`switch2(config)#`
	See id. at 930–31.

therewith, the remote hardware device information including a remote external port identifier of a remote external port that received the snooping information on the remote aggregation switch.	 *See id.* at 931. Additionally, in the exemplary, non-limiting configuration below, switch 2 (e.g., remote aggregation switch) includes port channel 20 of the MLAG 12. The port channel 20 of switch 2 bundles Ethernet interfaces 9 and 10. These Switch2 commands bundle Ethernet interfaces 9 and 10 in port channel 20, then associate that port channel with MLAG 12. ``` switch2(config)#interface ethernet 9-10 switch2(config-if-et9-10)#channel-group 20 mode active switch2(config-if-et9-10)#interface port-channel 20 switch2(config-if-po20)#mlag 12 switch2(config-if-po20)#exit switch2(config)# ```

	See id.  *See id.* In the Arista Switches, the snooping information including the unicast and multicast MAC addresses are synchronized between the MLAG peers.

Answered on September 26, 2015 2:29 am

IGMP snooping is responsible for installing multicast mac addresses in the mac address table. In MLAG, the unicast and multicast mac addresses are synchronized between the MLAG peers. If a snooping entry exists on an MLAG port-channel, traffic destined to that group will be sent to that MLAG port-channel from either peer switch. The decision of which switch to forward this traffic is made by an upstream device and its hashing. Once traffic arrives on one of the MLAG peers, we will always try to forward it out a local interface, if possible. Only once a mac address is learned on a non-MLAG port-channel or on a port-channel where the local interfaces are down, do we use the peer-link for forwarding.

See IGMPSnooping in MLAG, ARISTA NETWORKS, https://eos.arista.com/forum/igmpsnooping-in-mlag/ (last accessed April 30, 2021).

The peer link acts as an interface for the two switches to communicate with each other, and the snooping information is synchronized over the peer link.

A multi-chassis link aggregation group (MLAG) is a pair of links that terminate on two cooperating switches and appear as an ordinary link aggregation group (LAG). The cooperating switches are MLAG peer switches and communicate through an interface called a peer link. While the peer link's primary purpose is exchanging MLAG control information between peer switches, it also carries data traffic from devices that are attached to only one MLAG peer and have no alternative path. An MLAG domain consists of the peer switches and the control links that connect the switches.

See EOS 4.25.2F User Manual, ARISTA NETWORKS, https://www.arista.com/assets/data/pdf/user-manual/um-books/EOS-4.25.2F-Manual.pdf, at 920 (last accessed April 30, 2021).

In the Arista Switches, the snooping information shared by the remote aggregation switch includes the unicast and multicast MAC addresses that are mapped with the respective MLAG port channel (e.g., remote hardware device information). In MLAG, the snooping entries including the unicast and multicast MAC addresses are mapped with the respective MLAG port channels on the aggregation switch (including the remote aggregation switch) that received the snooping information. The port channels are specified by the p_range.

show mac address-table mlag-peer

The **show mac-address-table mlag-peer** command displays the specified MAC address table entries learned from the MLAG peer switch.

Command Syntax

```
show mac address-table mlag-peer [ENTRY_TYPE] [MAC_ADDR] [INTF_1 ...
INTF_N] [VLANS]
```

INTF_X command filters display by port list. When parameter lists multiple interfaces, command displays all entries containing at least one listed interface.

- <no parameter> all Ethernet and port channel interfaces.
- **ethernet** *e_range* Ethernet interfaces specified by *e_range*.
- **port-channel** *p_range* Port channel interfaces specified by *p_range*.

See id. at 1046.